Data Protection Guideline

Unruhe Privatstiftung

Contents

0. Preface

Trust is important, especially when it concerns your data. Thus, we see it as our duty to manage your data with the utmost care and to do everything in our power to protect your information from misuse.

Unruhe Privatstiftung ("Unruhe") strictly adheres to the data protection regulations pertaining to the collection and processing of your data. The following information will provide a detailed explanation of which data are processed and collected during your visit to our website and how we use said data.

This privacy policy applies to the company with all trading licenses (corporate consultancy) as well as Unruhe's websites (www.unruhestiftung.org and www.sozialmarie.org). Individual pages may contain links to other providers within or outside of the Unruhe enterprise, which the privacy policy does not cover. Thus, we cannot assume any liability for this content.

25.05.2018, Birgit Schörg, Isabel Albrecht, Josef Weber

1. Responsible bodies

Data protection management for data subjects, data protection violations, technical security, procedure log	The Board of Unruhe Privatstiftung
Order processor	See in-house directory
In-house data protection coordinator	Unruhe Privatstiftung, Mittersteig 13/6, 1040 Vienna, Tel. +43 1 58 77 181, Email: unruhe@ziel.at

2. Objective of the Data Protection Guideline

Within the scope of its corporate responsibility, Unruhe Privatstiftung ("Unruhe") undertakes to comply with data protection law. The protection of privacy is the foundation for trusting business relationships and for the reputation of Unruhe as an attractive employer and partner.

In addition, we define our own privacy objectives as a commitment. This includes:

- Absolute compliance with the provisions of the EU General Data Protection Regulation by the entire staff and all partners
- Absolute compliance with corporate privacy policies by the entire staff and all partners
- Strict obligation to secrecy and confidentiality
- Data protection compliant workplace design
- Absolute protection against the viewing of data by unauthorised persons

3. Scope of application and amendment to the Data Protection Guideline

This privacy policy is based on the provisions of the EU General Data Protection Regulation and the associated national laws.

This privacy policy applies to Unruhe at all current and future locations.

The latest version of the privacy policy can be requested free of charge and at any time from Unruhe Privatstiftung, Mittersteig 13/6, 1040 Vienna, Tel. +43 1 58 77 181, Email: unruhe@ziel.at.

4. What is personal data and what does processing mean?

Personal data refers to any information that identifies a natural or legal person.

The identifiability can be direct, indirect or attributable, as well as all classification to one or more special features that are an expression of the physical, physiological, genetic, economic, cultural or social identity of that natural or legal person. Examples of this personal data include: name (direct identifiability), "executive manager of" (indirect identifiability), address, date of birth, IP address, bank details, fingerprints, etc.

Processing means any procedure performed with or without the assistance of automated processes, or any operational sequence associated with personal data such as collecting, gathering, organising, filing, storing, adapting or modifying, selecting, querying, using, disclosing, communicating, disseminating or any other form of provision, comparison or linkage, restriction, erasure or destruction.

We process the personal data that we receive from you in the course of a business relationship. In addition, we process data that we have legitimately received from credit agencies, debtor directories and from publicly available sources (e.g., company register, club register, land register, media).

Personal data includes the following:

- Your personal details (name, address, contact details, date of birth, place of birth, citizenship etc.)
- Legitimisation data (e.g., identification data)
- Etc.

Furthermore, the following data may also be included:

- Submission data
- Data related to the fulfilment of our contractual obligation
- Information about your financial status (e.g., credit data)
- Advertising and sales data
- Documentation data (e.g., consulting protocols)
- Image and audio data (e.g., video or telephone recordings)
- Information from your electronic traffic with us (e.g., logins, cookies etc.)
- Processing results that we generate ourselves
- Data to adhere to legal and regulatory requirements
- Etc.

We process your personal data in accordance with the data protection regulations:

- for the fulfilment of contractual obligations (Art. 6 para. 1(b) GDPR):

  The processing of your data (personal data, Art. 4 No. 2 GDPR) is necessary in order to complete orders with you. We also need them to carry out our contracts as well as to execute your orders. We also process personally identifiable data in order to carry out activities necessary for the operation and administration of a corporate consultancy.

  The purposes of data processing are primarily based on the specific product and include, among others, requirement analysis, consulting, photographs, assessments.

- for the fulfilment of legal obligations (Art. 6 para. 1(c) GDPR): Certain statutory obligations to which Unruhe is subject may require the processing of personal data
- within the framework of your consent (Art. 6 para. 1(a) GDPR): If you have given us consent to process your personal data, processing will only take place in accordance with the purposes set out in the consent declaration and to the extent agreed therein. Any consent given may be revoked at any time with future effect (for example, you may object to the processing of your personal data for marketing and promotional purposes if you no longer consent to prospective processing).
- for the protection of legitimate interests (Art. 6 para. 1(f) GDPR): Should it be necessary, in order to protect legitimate interests of Unruhe or a third party, to process your data beyond the fulfilment of the contract, data processing will take place in the following cases:
  - Review and optimisation of procedures for requirement analysis and direct customer contact
  - Advertising or marketing and opinion research, insofar as you have not objected to the use of your data according to Art. 21 GDPR
  - Telephone records (e.g., in case of complaints)
  - Measures on business management and further development of services and products
  - Measures to protect employees, partners, customers and the property of Unruhe
  - Within the framework of taking legal action
  - Consultation and data exchange with credit agencies (e.g., Österreichischer Kreditschutzverband 1870) to identify credit risks and default risks

5. Disclosure of personal data – who receives your data?

Disclosure of personal data to recipients outside of Unruhe or to recipients within Unruhe is subject to the admissibility requirements of personal data processing. The recipient of the data must be obliged to only use the data for the specified purposes.

In the case of data disclosure to a recipient outside of Unruhe in a third country, this recipient must guarantee an equivalent level of data protection to this privacy policy. This does not apply if disclosure is due to statutory obligations.

In the case of data disclosure from third parties to Unruhe, it must be ensured that the data can be used for the intended purposes.

6. For what duration is your data stored?

Your data is stored for the duration of the entire business relationship (from initiation to settlement, up to termination of a contract) as well as in accordance with statutory retention and documentation obligations. These arise, among other things, from the Austrian Commercial Code (UGB).

In addition, regarding the storage duration, the statutory limitation periods, which can be up to 30 years in certain cases (the general limitation period is three years) e.g., under the General Civil Code (ABGB), must be taken into consideration.

7. Contract data processing (service provider)

Contract data processing takes place when a contractor is commissioned with the processing of personal data without being transferred the responsibility for the associated business process. In these cases, a contract data processing agreement must be concluded with external contractors.

The commissioning company retains full responsibility for the correct execution of the data processing. The contractor may only process personal data in accordance with the instructions of the client. Upon commissioning, the following requirements must be met and the commissioning department must ensure its implementation:

1. The contractor shall be selected according to its suitability to ensure the necessary technical and organisational protective measures.

2. The order is to be placed in written form. The data processing instructions and the responsibilities of the client and the contractor must be documented.

3. Before beginning data processing, the client must be satisfied with the fulfilment of the obligations by the contractor. Compliance with the data security requirements can be demonstrated by a contractor, in particular by submitting appropriate certification. Depending on the risk of data processing, inspection may need to be repeated regularly during the contract period.

4. In the case of cross-border contract data processing, the respective national requirements for the transfer of personal data abroad must be met. In particular, the processing of personal data outside of the European Economic Area in a third country may only take place if the contractor demonstrates a level of data protection equivalent to that of this Data Protection Guideline

5. Acknowledgement of binding company regulations of the contractor for the creation of an adequate level of data protection by the competent data protection supervisory authorities.

Appropriate contracts have been concluded with all contract processors and have been added to the processing directory. As soon as a new processor is added, a contract is signed.

8. Rights of data subjects

Every data subject can exercise the following rights. Enforcement must be processed immediately by the responsible department and may not lead to any disadvantages on the part of the data subject.

1. The data subject can request information about which personal data of which origin and which purpose is being stored. If further inspection rights are provided in documents (for example the personal file) of the employment relationship and in accordance with labour law, these remain unaffected.

2. If personal data is disclosed to third parties, information must also be provided regarding the identity of the recipient or categories of recipients.

3. If personal data is incorrect or incomplete, the data subject may request the correction or supplementation thereof.

4. The data subject can object to the processing of his/her personal data for the purposes of advertising, marketing or opinion polling. The data must be blocked for this purpose.

5. The data subject is entitled to request the erasure of his/her data if the legal basis for the processing of the data is missing or has been removed. The same applies if the purpose of the data processing has expired due a lapse of time or other reasons. Existing storage requirements and deletion of contrasting legitimate interests must be observed.

6. The data subject has a fundamental right of objection to the processing of his/her data, which must be considered if his/her legitimate interest outweighs the interest of processing due to a special personal situation. This does not apply if there is a legal provision to carry out the processing.

You can also submit complaints to the Austrian Data Protection Authority (www.dsb.gv.at).

9. Are you obligated to provide data?

You must provide all personal data that is required to establish and execute our business relationship and to which we are obligated by law.

If you do not want to provide us with the data, we generally have to reject contract conclusion or order execution. In this case, we can no longer execute an existing contract and consequently have to terminate it.

However, you are not obligated to give consent for the processing of data that is not relevant for the fulfilment of the contract or required by law and/or regulatorily required.

10. Data processing confidentiality

Personal data is subject to data secrecy. Unauthorised collection, processing or use is prohibited for employees/partners.

Any processing carried out by an employee/partner, without being tasked with the fulfilment of his/her duties and being entitled to do so, is unauthorised. The need-to-know principle applies: employees/partners may only access personal data if and to the extent necessary for their respective

tasks. This requires the careful allocation and division of roles and responsibilities as well as their implementation and maintenance in the context of authorisation concepts.

Employees/partners may not use personal data for their own private or commercial purposes, transmit said data to unauthorised persons or make it accessible in any other way.

11. Data processing safety/security

Personal data must be protected against unauthorised access, unlawful processing or disclosure, as well as against loss, falsification or destruction at all times. This applies regardless of whether the data processing is done electronically or in paper form. Before introducing new data processing techniques, in particular new IT systems, technical and organisational measures for the protection of personal data must be established and implemented. These measures must be based on state-of-the-art technology, the risks posed by processing, and the need for the protection of the data (as determined by the information classification process).

The technical organisational measures for the protection of personal data are part of the company-wide information security and data protection management and must continuously be adapted to the technical developments and organisational changes.

Employees/partners are prohibited from processing personal data outside of the services and processes provided by Unruhe (programmes, shelves, etc.), as well as outside of comprehensible and legitimate contracts.

12. Cookies, retargeting, web analytics

To make our services as pleasant as possible, we use so-called cookies. Cookies are small text files that allow the user to be recognised upon return. You can prevent the installation of cookies by setting your browser software accordingly.

We have commissioned different service providers (Adobe, Sizmek, Google, Adform, Netzffekt) to create cookies on the websites of www.unruhestiftung.org and www.sozialmarie.org in order to analyse the structure and navigation of our websites, to improve them and tailor them to the needs of our customers and to provide you with customised promotional offers based on your individual needs. Our service providers only receive anonymous data and are not able to establish a connection to your person.

As a result, Unruhe receives statistical evaluations, with which we review the need-based design of our website.

Please note that if you object to these cookies, not all the functions of our website will be available in their entirety. By using this website, you agree to the processing of the data collected about you by our service providers.

13. Social media

Unruhe cooperates with various social network providers. As part of this collaboration, your browser automatically connects to the selected service provider (e.g., Facebook) when using the respective service. Thereby, for example, your IP address, cookies and other information will be transmitted to the service provider if you have previously visited its website. This data transmission is prevented as much as possible and only takes place when you interact with the social network. If you are logged into

the corresponding platform of the social network, it can assign your visit to our website to your user account.

We also use plug-ins (for example, Facebook-Symbol) of various platforms. By clicking on the symbol, you agree to the communication with the respective platform and the transmission of information (for example, your IP address) to the respective service provider. For further information on the respective use of your data, please refer to the privacy policy of the selected service provider.

Facebook's privacy policy can be found here:

www.facebook.com/legal/terms/customaudience and under

www.facebook.com/legal/terms/businesstools

14. Data protection monitoring

Compliance with the date protection guidelines and applicable privacy laws is regularly monitored through privacy audits and other monitoring measures.

The monitoring results must be reported to management.

15. Data protection incidents (data protection breaches)

Every employee/partner must immediately report breaches of this privacy policy or other provisions on the protection of personal data (date protection incidents) to management.

In cases of

- unauthorised or unlawful processing of personal data,
- accidental or unlawful destruction,
- accidental or unlawful loss,
- accidental or unlawful amendment, and
- accidental or unlawful disclosure.

16. Responsibilities and sanctions

Management is responsible for the compliant processing of personal data.

Thus, management is obliged to ensure that data protection and privacy requirements of the Data Protection Guideline are adhered to (e.g., national reporting requirements).

It is management's task to ensure proper data processing while taking data protection into account, through organisational, personnel and technical measures. The implementation of these specifications is the responsibility of the competent employee/partner. The data protection officer must be informed immediately about audits by authorities.

The following areas must be checked to see if the appointment of a data protection officer is obligatory: company size/number of employees/partners, processing of sensitive data, area of business.

It may occur that Unruhe receives sensitive data from submitters for (social) projects. This happens very rarely; therefore, Unruhe does not need a data protection officer in accordance with the abovementioned conditions. Should any of these conditions change, a data protection officer will be appointed immediately.

The data protection management (this refers to the Board of Unruhe) is the contact person on location for data protection. It can perform reviews and must familiarise the employees/partners with the contents of the Data Protection Guideline. Those responsible for business processes and projects must inform the data protection management in good time about new processing of personal data. In the case of data processing undertakings, which may result in particular risks to the personal rights of data subjects, data protection management must be involved even before processing begins. This particularly applies to personal data that is especially worthy of protection.

Management must ensure that its employees/partners are trained to the extent necessary for proper data protection.

Violations, for which individual employees/partners are responsible, can lead to labour law sanctions.

Data protection management: Unruhe Privatstiftung, Mittersteig 13/6, 1040 Vienna, Tel. +43 1 58 77 181, Email: unruhe@ziel.at

17. The data protection coordinator

The data protection coordinator implements the privacy policy provisions and supports privacy management in complying with data protection regulations. The data protection coordinator will inform the Board in a timely manner about changes in the area of data protection.

Any data subject can contact the data protection coordinator or data protection management about suggestions, inquiries, requests for information, or complaints related to privacy or data security issues. On request, inquiries and complaints are treated confidentially.

In-house data protection coordinators: Unruhe Privatstiftung, Mittersteig 13/6, 1040 Vienna, Tel. +43 1 58 77 181, Email: unruhe@ziel.at

18. Enactment

This document is reviewed annually and, as required, also for completeness and timeliness.

Amendments to this document are the responsibility of the competent privacy management body.

This document must be accessible to all employees/partners.